CLAIMS

What is claimed is:

1. A security analysis tool for an automation system, comprising:

an interface component to generate a description of factory assets; and

an analyzer component to generate one or more security outputs based on the description.

2. The tool of claim 1, at least one of the interface component and the analyzer component operate on a computer and receive one or more factory inputs that provide the description.

3. The tool of claim 2, the factory inputs include user input, model inputs, schemas, formulas, equations, files, maps, and codes.

4. The tool of claim 2, the factory inputs are processed by the analyzer component to generate the security outputs, the security outputs including at least one of manuals, documents, schemas, executables, codes, files, e-mails, recommendations, topologies, configurations, application procedures, parameters, policies, rules, user procedures, and user practices that are employed to facilitate security measures in an automation system.

5. The tool of claim 1, the interface component includes at least one of a display output having associated display objects and at least one input to facilitate operations with the analyzer component, the interface component is associated with at least one of an engine, an application, an editor tool, a web browser, and a web service.

6. The tool of claim 5, the display objects include at least one of configurable icons, buttons, sliders, input boxes, selection options, menus, and tabs, the display objects having multiple configurable dimensions, shapes, colors, text, data and sounds to facilitate operations with the analyzer component.

7. The tool of claim 5, the at least one inputs includes receiving user commands from a mouse, keyboard, speech input, web site, remote web service, camera, and video input to affect operations of the interface component and the analyzer component.

8. The tool of claim 1, the description includes a model of one or more automation assets to be protected and associated network pathways to access the automation assets.

9. The tool of claim 1, the description includes at least one of risk data and cost data that is employed by the analyzer component to determine suitable security measures.

10. The tool of claim 1, the description includes at least one of shop floor access patterns, Intranet access patterns, Internet access patterns, and wireless access patterns.

11. The tool of claim 1, the analyzer component is adapted for partitioned security specification entry and sign-off from various groups.

12. A security analysis method, comprising:

inputting a at least one model related to one or more factory assets; and

generating one or more security outputs based on the model.

13. The method of claim 12, the at least one model is related to at least one of a risk-based model and a cost-based model.

14. The method of claim 12, the security outputs include at least one of recommended security components, codes, parameters, settings, related interconnection topologies, connection configurations, application procedures, security policies, rules, user procedures, and user practices.

15. The method of claim 12, further comprising at least one of:

automatically deploying the security outputs to one or more entities; and

utilizing the security outputs to mitigate at least one of unwanted network access and network attack.

16. A security analysis system in an automation environment, comprising:

means for receiving abstract descriptions of at least one of factory assets and network devices; and

means for generating one or more security outputs based on the abstract description; and

means for automatically distributing the security outputs to facilitate network security in the automation environment.

17. A security validation system, comprising:

a scanner component to automatically interrogate an automation system at periodic intervals for security related data; and

a validation component to automatically assess security capabilities of the automation system based upon a comparison of the security related data and one or more predetermined security guidelines.

18. The system of claim 17, the scanner component and the validation component are at least one of a host-based component and a network-based component.

19. The system of claim 17, the validation component performs at least one of a security audit, a vulnerability scan, a revision check, an improper configuration check, file system check, a registry check, a database permissions check, a user privileges check, a password check, and an account policy check.

20. The system of claim 17, the security guidelines are automatically determined.

21. The system of claim 18, the host-based component performs vulnerability scanning and auditing on devices, the network-based component performs vulnerability scanning and auditing on networks.

22. The system of claim 21, at least one of host-based component and the network-based component at least one of determines susceptibility to common network-based attacks, searches for open TCP/UDP ports, scans for vulnerable network services, attempts to gain identity information about end devices that relates to hacker entry, performs vulnerability scanning and auditing on firewalls, routers, security devices, and factory protocols.

23. The system of claim 21, at least one of host-based component and the network-based component at least one of includes non-destructively mapping a topology of IT and automation devices, checking revisions and configurations, checking user attributes, and checking access control lists.

24. The system of claim 17, further comprising a component to automatically initiate a security action in response to detected security problems.

25. The system of claim 24, the security action includes at least one of automatically correcting security problems, automatically adjusting security parameters, altering network traffic patterns, add security components, removing security components, firing alarms, automatically notifying entities about detected problems and concerns, generating an error or log file, generating a schema, generating data to re-configure or re-route network connections, updating a database, and updating a remote site.

26. An automated security validation method, comprising:

scanning one or more networks or automation devices for potential security violations; and

performing an automated security procedure if a security violation is detected.

27. The method of claim 26, further comprising at least one of:

checking for susceptibility to network-based attacks;

searching for open TCP/UDP ports; and

scanning for vulnerable network services.

28. The method of claim 26, further comprising at least one of:

automatically performing security assessments;

automatically performing security compliance checks; and

automatically performing security vulnerability scanning.

29. The method of claim 26, the automated security procedures include at least one of automatically performing corrective actions, altering network patterns, adding security components, removing security components, adjusting security parameters, and generating security data to mitigate network security problems.

30. An automated security validation system, comprising:

means for scanning one or more networks or automation devices for potential security violations;

means for initiating a security procedure in response to the security violations; and

means for performing at least one of security assessments, security compliance checks; and security vulnerability scanning to mitigate the security violations.

31. A security learning system for an automation environment, comprising:

a learning component to monitor and learn automation activities during a training period; and

a detection component to automatically trigger a security event based upon detected deviations of subsequent automation activities after the training period.

32. The system of claim 31, the automation activities includes at least one of a network activity and a device activity.

33. The system of claim 31, the learning component including at least one of a learning model and a variable

34. The system of claim 31, the automation activities include at least one of a number of network requests, a type of network requests, a time of requests, a location of requests, status information, and counter data.

35. The system of claim 31, the detection component employs at least one of a threshold and a range to determine the deviations.

36. The system of claim 35, the threshold and the range are dynamically adjustable.

37. The system of claim 33, the learning model includes at least one of mathematical models, statistical models, probabilistic models, functions, algorithms, and neural networks, classifiers, inference models, Hidden Markov Models (HMM), Bayesian models, Support Vector Machines (SVM), vector-based models, and decision trees.

38. The system of claim 31, the security event includes at least one of automatically performing corrective actions, altering network patterns, adding security components, removing security components, adjusting security parameters, firing an alarm, notifying an entity, generating an e-mail, interacting with a web site, and generating security data to mitigate network security problems.

39. A security learning method, comprising:

monitoring a network for a predetermined time;

automatically learning at least one data pattern during the predetermined time; and

generating an alarm if a current data pattern is determined to be outside of a predetermined threshold associated with the at least one data pattern.

40. The method of claim 39, the at least one data pattern employed as input for a security analysis process.

41. A security learning system in an automation environment, comprising:

means for scanning a network;

means for learning data patterns from the network; and

means for generating a security event if current data patterns are determined to be out of tolerance from stored data patterns.

42. A security schema for a factory automation system, comprising:

a first data field to describe device security parameters;

a second data field to describe network security parameters;

a third data field to describe security guidelines; and

a schema to represent the data fields, the schema employed to mitigate network security problems in the factory automation system.

43. The schema of claim 42, the schema is processed in an at least one of an XML format and an SQL format.

44. The schema of claim 42, further comprising at least one of a recommendations element, a topologies element, a configurations element, an application procedures element, a policies element, a rules element, and a user procedures element to mitigate network security problems.